## REMARKS/ARGUMENTS

The Examiner rejects claims 1-8, 10-18, 20-21, 23-25, 27-28, and 30 under 35 U.S.C.§102(e) as being anticipated by Davis (U.S. 2003/0016653); claims 9, 26, and 29 under 35 U.S.C.§103(a) as being unpatentable in view of Davis and further in view of Wan et al. (U.S. 6,529,475); and claims 19 and 22 under 35 U.S.C.§103(a) as being unpatentable in view of Davis and further in view of Bar et al. (U.S. 6,122,665).

Claims 1-30 have been canceled, rendering the rejections moot.

New claims 31-56 have been added. To facilitate prosecution, Applicant respectfully submits that the newly added claims are allowable over the cited references. The cited references fail to teach, individually or collectively, at least the following italicized features of the newly added independent claims:

> 31. A method for identifying a corresponding session for a packet, comprising:
>
> (a) *in a first session, a first endpoint transmitting first and second sets of packets, respectively, to a session monitor and a second endpoint, wherein the first and second sets of packets have differing memberships, wherein each packet in the first set of packets is used for determining network performance information, and wherein each of the first and second endpoints have an associated electronic address on a network and a session identifier;*
>
> (b) the session monitor receiving at least a first packet in the first packet set, *the first packet comprising at least the network address and session identifier associated with the first endpoint*;
>
> (c) determining whether at least one of the first endpoint's network address *and session identifier* correspond to an active session entry recorded in a first set of data structures, the first set of data structures comprising active session entries, each entry in the first set of data structures having at least network addresses for each of the endpoints to the corresponding session;
>
> (d) *when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the first set of data structures, updating the corresponding entry to include the network performance information associated with the at least a first packet;*
>
> (e) *determining whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a second set of data structures, the second set of data structures having active session entries, each of the entries in the second set of data structures failing to comprise network addresses for each*

*of the endpoints to the corresponding session*; and

(f) *when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the second set of data structures, updating the entry to include the performance information associated with the at least a first packet.*

40. In a network, the network comprising:

(i) a session monitor operable to track network performance for a plurality of sessions; and

(ii) *first endpoint and second endpoints, the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint, wherein the first and second sets of packets have differing memberships, wherein each packet in the first set of packets is used by the session monitor to determine network performance information, and wherein each of the first and second endpoints have an associated electronic address on a network and a session identifier*, the session monitor comprising:

(a) an input operable to receive at least a first packet in the first packet set, the first packet comprising at least the network address *and session identifier* associated with the first endpoint; and

(b) a matcher operable to:

(b1) determine whether at least one of the first endpoint's network address *and session identifier* correspond to an active session entry recorded in a first set of data structures, the first set of data structures comprising active session entries, each entry in the first set of data structures having at least network addresses for each of the endpoints to the corresponding session;

(b2) *when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the first set of data structures, update the corresponding entry to include the performance information associated with the at least a first packet;*

(b3) *determine whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a second set of data structures, the second set of data structures having active session entries, each of the entries in the second set of data structures failing to comprise network addresses for each of the endpoints to the corresponding session*; and

(b4) *when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the second set of data structures, update the entry to include the performance information associated with the at least a first packet.*

48. In a network, the network comprising:

(i) a session monitor operable to track network performance for a plurality of sessions; and

(ii) *first endpoint and second endpoints, the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint, wherein the first and second sets of packets have differing memberships, wherein each packet in the first set of packets is used by the session monitor to determine*

*network performance information, and wherein each of the first and second endpoints have an associated electronic address on a network and a session identifier*, a method comprising:

(a) the first endpoint receiving at least a first packet communicated between the first endpoint and a second endpoint to a first session, the first packet comprising an address of the first endpoint on the network, an address of the second endpoint on the network, and voice information, and being a member of the second packet set; and

(b) *the first endpoint transmitting at least a second packet to a session monitor, the at least a second packet including the respective first and second network addresses of the first and second endpoints and being a member of the first packet set.*

51. In a network, the network comprising:

(i) a session monitor operable to track network performance for a plurality of sessions; and

(ii) *first endpoint and second endpoints, the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint, wherein the first and second sets of packets have differing memberships, wherein each packet in the first set of packets is used by the session monitor to determine network performance information, and wherein each of the first and second endpoints have an associated electronic address on a network and a session identifier*, the first endpoint comprising:

(a) an input operable to receive at least a first packet communicated between the first and second endpoints to a first session, the first packet comprising a network address of the first endpoint, a network address of the second endpoint, and voice information, and being a member of the second packet set; and

(b) *a transmitter operable to transmit at least a second packet to a session monitor, the at least a second packet including the respective first and second network addresses of the first and second endpoints and being a member of the first packet set.*

54. A session packet for transmission on a network, comprising:

a source network address of a first participant to a Voice over Internet Protocol (VoIP) session;

*a destination network address associated with a session monitor*;

*a network address of a second participant to the VoIP session*; and

session information associated with the VoIP session.

The claimed invention is particularly advantageous for Voice over Internet Protocol or VoIP voice calls. A common architecture for VoIP is to have a session monitor in addition to each endpoint to effect session management. To enable the monitor to obtain RTCP packets, a dual unicast architecture has been developed. In dual unicast, one session participant (A)

transmits both RTP and RTCP packets to the other session participant (B) and RTCP packets to the monitor. Dual unicast, however, exposes design limitations in the RTCP protocol itself. Although endpoint session ids are unique to a particular (first) session (such as between A and B), an endpoint in a concurrent (second) session (such as between C and D) can have the same session id or synchronization source id ("SSRC") as an endpoint (A or B) in the other (first) session. When duplicate endpoint session ids are concurrently in use, the monitor can have substantial difficulty determining which RTCP packets correspond to which session, potentially causing inaccurate performance analysis.

In one embodiment, the claimed invention addresses this problem by maintaining a listing of network addresses and/or session identifiers to track active RTP sessions. When an RTCP packet is received, the network address and/or session identifier of the source endpoint matches an entry in the listing, a network address of the destination endpoint is determined. The listing can cause the window of opportunity for confusing concurrent sessions and attributing data in RTCP packets to the wrong session to be much smaller than with current architectures. The window of opportunity for possible confusion using the above algorithm(s) exists only when two different endpoints join different sessions at the same time and with the same SSRC. This window of opportunity or startup interval closes once either of the endpoints (or their peers) has sent an RTCP packet with a reception block corresponding to either endpoint. Once the reception block is exchanged, the SSRCs of both parties to the session are known to the monitor. Before such an exchange, the monitor typically has only the SSRC and network address of one party to the session. The SSRC and network address of the other party is unknown. The startup interval is typically fairly short, *e.g.*, typically on the order of 5 seconds or less. The use of the active session table and network address to define the session (rather than only pairings of

SSRCs) can, after the startup interval, at least substantially eliminate misinterpretation of RTCP packets and incorrect analysis of performance data. The accuracy of the algorithm(s) in matching RTCP packets with the corresponding session results in more accurate statistical analysis of the communication link in the network.

Davis

Davis, the primary reference, is directed to a method and system for identifying sessions between two networked computers. Each packet exchanged between the computers includes information relating to the computers, typically in an IP five-tuple, that is used to route the packet to the appropriate computer system. The IP five-tuple includes five fields, namely the protocol 32, two source fields 34 and 36 (i.e., the source address and port) and two destination fields 38 and 40 (i.e., the destination address and port). To keep track of the active sessions, a session table is maintained at a router, such as routers 2 and 16. An asymmetric key is obtained by concatenating the fields 32, 34, 36, and 38 of the IP five-tuple for the packet. The key is then used to search the session table 50 for the index which matches the key. Davis makes the key symmetrical by arithmetic manipulation of the IP five-tuple fields. In other words, the key is the same regardless of whether the packet is traveling from the first computer to the second computer or vice versa. The algorithm sums selected pairs of the four fields, concatenates the sums, and determines an absolute value of a difference between the sums. The absolute value is the key.

Davis fails to teach or suggest a number of features including:

(a) the use of dual unicast to provide packets containing performance metrics both to an endpoint and monitor at different addresses;

(b) the joint use of an active session table 308 (of first set of data structures) containing a listing of matched session endpoints and orphan table 304 (or second set of data structures)

containing a listing of unmatched session endpoints or orphans; and/or

(c) an orphan table containing a transport address of a first session endpoint, an identifier of the endpoint, and associated performance information associated with the packet, such as jitter, packet loss, and round-trip time, related to the session.

Wan et al.

Wan et al. is directed to an architecture for reducing congestion of real time data traffic on a multimedia communications network having a traffic control mechanism. The method includes the step of first extracting from data traffic in the multimedia communications network information regarding congestion of the multimedia communications network. This extraction is performed by a network of monitors. Secondly, congestion is regulated by a central server that receives network information from the monitors and uses the information to analyze congestion status and communicate instructions to the multimedia communications network to reduce congestion.

Bar et al.

Bar, et al., is directed to a system and method for monitoring a computer network to detect data packets including audio or video data, such as packets being part of a communication session, for storing the packets and for reconstructing the communication session upon request.

Accordingly, the pending claims are allowable.

The dependent claims provide further reasons for allowance.

By way of example, dependent claims 32 and 41 require, *inter alia*, entry matching the first and second sets of data structures to be performed using a pairing of network address and session identifier for a selected endpoint. Davis, et al., fails to performing matching based on an

address and endpoint identifier pair. Rather, Davis, et al., uses, for entry matching, an asymmetric key obtained by concatenating the fields 32, 34, 36, and 38 of the IP five-tuple for the packet.

Dependent claims 33, 38, 42, and 47 require that the second set of data structures not be matching against when the incoming packet contains the network addresses of both endpoints.

Dependent claims 34 and 43 require that session entries in the second set of data structures that correspond to a common session, when identified, be removed from the second set of data structures and moved to the first set of data structures.

Dependent claims 37 and 46 require the first set of data structures to include, for each active session, a transport address of each of the endpoints participating in the session, the session identifiers for each of the endpoints participating in the session, and performance information corresponding to packets exchanged in the session, the second set of data structures to include, for each active session, a transport address of at least one of the endpoints participating in the session, a session identifier for at least one but less than all of the endpoints participating in the session, and performance information corresponding to packets exchanged in the session, the performance information to include at least one of jitter, packet loss, and packet round-trip time, the media information to include voice data, and the packets in the first set of packets to exclude media information.

Dependent claims 49 and 52 require the flag value in an incoming first packet to determine whether or not to send a second packet to a session monitor. Although Bar, et al., teaches setting a flag for "start session request" and for "wait for logic channel", it does not teach setting a flag to determine whether or not to forward a packet to a monitor.

Based upon the foregoing, Applicants believe that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

By: Douglas Swartz

Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: Dec. 23, 2005